



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년01월14일
(11) 등록번호 10-2755149
(24) 등록일자 2025년01월10일

(51) 국제특허분류(Int. Cl.)
G06K 19/06 (2006.01)
(52) CPC특허분류
G06K 19/06037 (2013.01)
G06K 19/06028 (2013.01)
(21) 출원번호 10-2023-0107783
(22) 출원일자 2023년08월17일
심사청구일자 2023년08월17일
(56) 선행기술조사문헌
KR1020230092744 A
비특허문헌1
비특허문헌2
KR101572870 B1

(73) 특허권자
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
나준희
세종특별자치시 마은안1로 125, 53호 (고운동)
김기태
대전광역시 서구 만년로68번길 58, 102동 411호
(만년동, 시티팰리스)
(74) 대리인
이재명

전체 청구항 수 : 총 11 항

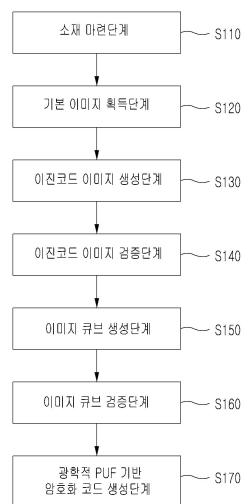
심사관 : 이종환

(54) 발명의 명칭 광학적 PUF 기반 암호화 코드 획득 방법 및 이를 이용하여 획득되는 광학적 PUF 기반 암호화 코드

(57) 요약

본 발명의 일실시예는 반도체 기반 PUF와는 다른 광학적 PUF 기반 암호화 코드 획득 방법 및 이를 이용하여 획득되는 광학적 PUF 기반 암호화 코드를 제공한다. 여기서, 광학적 PUF 기반 암호화 코드 획득 방법은 굴절률 이방성 소재를 마련하는 단계와, 굴절률 이방성 소재에 빛을 투과시키고, 굴절률 이방성 소재를 투과한 빛을 수광하여 간섭 패턴을 가지는 기본 이미지를 획득하는 단계와, 간섭 패턴에 대응되는 이진코드를 가지는 이진코드 이미지를 생성하는 단계와, 복수개의 이진코드 이미지를 적층하여 이미지 큐브를 생성하는 단계와, 이미지 큐브에서 복수 개의 이진코드 이미지를 포함하는 면을 선정하고, 면에서 이진코드를 추출하여 광학적 PUF 기반 암호화 코드를 생성하는 단계를 포함한다.

대표도 - 도1



(52) CPC특허분류

G06K 19/06046 (2013.01)

H04L 9/3278 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711180119
과제번호	2021R1A4A1032762
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	기초연구실지원사업(BRL)
연구과제명	멀티스케일 광제어 기초연구실
기 여 율	1/1
과제수행기관명	충남대학교
연구기간	2021.06.01 ~ 2024.02.29

명세서

청구범위

청구항 1

굴절률 이방성 소재를 마련하는 소재 마련단계;

상기 굴절률 이방성 소재에 빛을 투과시키고, 상기 굴절률 이방성 소재를 투과한 빛을 수광하여 간섭 패턴을 가지는 기본 이미지를 획득하는 기본 이미지 획득단계;

상기 간섭 패턴에 대응되는 이진코드를 가지는 이진코드 이미지를 생성하는 이진코드 이미지 생성단계;

복수개의 상기 이진코드 이미지를 적층하여 이미지 큐브를 생성하는 이미지 큐브 생성단계; 및

상기 이미지 큐브에서 복수 개의 상기 이진코드 이미지를 포함하는 면을 선정하고, 상기 면에서 이진코드를 추출하여 광학적 PUF 기반 암호화 코드를 생성하는 암호화 코드 생성단계를 포함하는 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 2

제1항에 있어서,

상기 굴절률 이방성 소재는 배향 공정을 거치지 않은 액정성 소재인 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 3

제1항에 있어서,

상기 굴절률 이방성 소재는 주름을 가지고,

상기 간섭 패턴은 상기 주름에 대응되게 형성되는 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 4

제1항에 있어서,

상기 기본 이미지 획득단계에서, 상기 기본 이미지는 상기 굴절률 이방성 소재를 사이에 두고 배치되는 교차 편광판을 통과한 빛을 수광하여 획득되고,

상기 기본 이미지는 상기 굴절률 이방성 소재를 기준으로 상기 교차 편광판의 회전 각도에 따라 무작위한 간섭 패턴을 가지는 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 5

제1항에 있어서,

상기 암호화 코드 생성단계에서,

상기 면은 상기 이미지 큐브 중의 무작위로 선정되는 3개의 점에 의해 형성되는 2차원의 면인 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 6

제5항에 있어서,

상기 면은 상기 이미지 큐브에서 복수 개의 상기 이진코드 이미지가 적층되어 형성되는 적층 표면에서 선정되는 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 7

제5항에 있어서,

상기 면은 상기 이미지 큐브의 내부에서 선정되는 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 8

제1항에 있어서,

상기 암호화 코드 생성단계에서,

상기 면은 상기 이미지 큐브 중의 무작위로 선정되는 4개 이상의 점에 의해 형성되는 3차원의 도형의 표면 중 하나 이상인 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 9

제1항에 있어서,

상기 간섭패턴에 대응되는 이진코드를 기초로 상기 이진코드 이미지의 무작위성을 검증하는 이진코드 이미지 검증단계를 포함하는 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 10

제1항에 있어서,

상기 이미지 큐브의 무작위성, 유일성 및 신뢰성을 검증하는 이미지 큐브 검증단계를 포함하는 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법.

청구항 11

제1항 내지 제10항 중 어느 하나의 항에 기재된 광학적 PUF 기반 암호화 코드 획득 방법을 이용하여 획득되는 광학적 PUF 기반 암호화 코드.

발명의 설명

기술 분야

[0001] 본 발명은 광학적 PUF 기반 암호화 코드 획득 방법 및 이를 이용하여 획득되는 광학적 PUF 기반 암호화 코드에 관한 것으로, 더욱 상세하게는 반도체 기반 PUF와는 다른 광학적 PUF 기반 암호화 코드 획득 방법 및 이를 이용하여 획득되는 광학적 PUF 기반 암호화 코드에 관한 것이다.

배경 기술

[0002] 최근 인터넷과 연결된 디지털 기술이 발전하고 있다. 사물 인터넷(IoT, Internet Of Things), 빅데이터, 클라우드 컴퓨팅 등과 같은 기술은 스마트폰, 스마트 카드 및 많은 유비쿼터스 전자기기와 가전 제품을 포함하는 복잡한 디지털 네트워크를 형성하고 있다. 결과적으로 삶과 관련된 많은 양의 디지털 정보가 매일 생성, 저장 및 전달되고 있다.

[0003] 하지만 이러한 디지털 정보는 높은 수준의 정보 보안 시스템이 마련되지 않는 한 보안에 취약하다. 정보 보안 시스템의 가장 중요한 측면 중 하나는 정보에 대한 접근을 원하는 단체 또는 개인의 인증이다. 이러한 인증 프로토콜은 일반적으로 지문과 같이 특별하고 복제할 수 없는 디지털 서명이다.

[0004] 최근 정보 보안 시스템의 대안으로 물리적 복제 방지 기술(PUF: Physical Unclonable Function, 이하 'PUF'라 한다)에 대한 연구가 활발히 진행되고 있다.

[0005] PUF는 반도체 칩의 제조공정 특성에 따라 나타나는 각 반도체 칩의 고유한 특징에서 유래되었으며, 하드웨어적으로 예측 불가능한 값이 출력되므로 복제가 불가능하다. 이러한 특성을 활용하여 Arbiter-PUF, RO(Ring Oscillator)-PUF, LoopPUF, VIA PUF 등 많은 종류의 PUF에 대한 연구 결과가 존재한다.

[0006] 그러나, 기존의 반도체 기반 PUF는 물리적으로 교체하거나 추가 하드웨어 구성요소가 필요한데, 이러한 필요 없이도 구현될 수 있는 PUF 기술과, 이러한 PUF 기술을 이용한 암호화 코드 획득 기술이 요구된다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 공개특허공보 제2022-0000815호(2022.01.04. 공개)

발명의 내용

해결하려는 과제

[0008] 상기와 같은 문제점을 해결하기 위하여, 본 발명이 이루고자 하는 기술적 과제는 반도체 기반 PUF와는 다른 광학적 PUF 기반 암호화 코드 획득 방법 및 이를 이용하여 획득되는 광학적 PUF 기반 암호화 코드를 제공하는 것이다.

[0009] 본 발명이 이루고자 하는 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 상기 기술적 과제를 달성하기 위하여, 본 발명의 일실시예는 굴절률 이방성 소재를 마련하는 소재 마련단계; 상기 굴절률 이방성 소재에 빛을 투과시키고, 상기 굴절률 이방성 소재를 투과한 빛을 수광하여 간섭 패턴을 가지는 기본 이미지를 획득하는 기본 이미지 획득단계; 상기 간섭 패턴에 대응되는 이진코드를 가지는 이진코드 이미지를 생성하는 이진코드 이미지 생성단계; 복수개의 상기 이진코드 이미지를 적층하여 이미지 큐브를 생성하는 이미지 큐브 생성단계; 및 상기 이미지 큐브에서 복수 개의 상기 이진코드 이미지를 포함하는 면을 선정하고, 상기 면에서 이진코드를 추출하여 광학적 PUF 기반 암호화 코드를 생성하는 암호화 코드 생성단계를 포함하는 것을 특징으로 하는 광학적 PUF 기반 암호화 코드 획득 방법을 제공한다.

[0011] 본 발명의 실시예에 있어서, 상기 굴절률 이방성 소재는 배향 공정을 거치지 않은 액정성 소재일 수 있다.

[0012] 본 발명의 실시예에 있어서, 상기 굴절률 이방성 소재는 주름을 가지고, 상기 간섭 패턴은 상기 주름에 대응되게 형성될 수 있다.

[0013] 본 발명의 실시예에 있어서, 상기 기본 이미지 획득단계에서, 상기 기본 이미지는 상기 굴절률 이방성 소재 사이에 두고 배치되는 교차 편광판을 통과한 빛을 수광하여 획득되고, 상기 기본 이미지는 상기 굴절률 이방성 소재를 기준으로 상기 교차 편광판의 회전 각도에 따라 무작위한 간섭 패턴을 가질 수 있다.

[0014] 본 발명의 실시예에 있어서, 상기 암호화 코드 생성단계에서, 상기 면은 상기 이미지 큐브 중의 무작위로 선정되는 3개의 점에 의해 형성되는 2차원의 면일 수 있다.

[0015] 본 발명의 실시예에 있어서, 상기 면은 상기 이미지 큐브에서 복수 개의 상기 이진코드 이미지가 적층되어 형성되는 적층 표면에서 선정될 수 있다.

[0016] 본 발명의 실시예에 있어서, 상기 면은 상기 이미지 큐브의 내부에서 선정될 수 있다.

[0017] 본 발명의 실시예에 있어서, 상기 암호화 코드 생성단계에서, 상기 면은 상기 이미지 큐브 중의 무작위로 선정되는 4개 이상의 점에 의해 형성되는 3차원의 도형의 표면 중 하나 이상일 수 있다.

[0018] 본 발명의 실시예에 있어서, 상기 간섭패턴에 대응되는 이진코드를 기초로 상기 이진코드 이미지의 무작위성을 검증하는 이진코드 이미지 검증단계를 포함할 수 있다.

[0019] 본 발명의 실시예에 있어서, 상기 이미지 큐브의 무작위성, 유일성 및 신뢰성을 검증하는 이미지 큐브 검증단계를 포함할 수 있다.

[0020] 한편, 상기 기술적 과제를 달성하기 위하여, 본 발명의 일실시예는 광학적 PUF 기반 암호화 코드 획득 방법을 이용하여 획득되는 광학적 PUF 기반 암호화 코드를 제공한다.

발명의 효과

- [0021] 본 발명의 실시예에 따르면, 액정 분포의 무작위성과 액정의 광학적 효과를 활용하여 지문과 같은 특정 패턴 코드를 형성할 수 있는 광학적 PUF 기반 기본 이미지를 제작할 수 있다.
- [0022] 또한, 본 발명의 실시예에 따르면, 기존의 반도체 기반 PUF와 달리 물리적으로 교체하거나 추가 하드웨어 구성 요소가 필요 없이 PUF 구성이 가능하다.
- [0023] 또한, 본 발명의 실시예에 따르면, 광학적 PUF 기반 기본 이미지의 자유형 모양의 무작위한 방향의 주름은 물리적으로 복제할 수 없는 형태이다. 따라서, 광학적 PUF 기반 기본 이미지를 이용하여 생성되는 광학적 PUF 기반 이진코드 이미지와, 이진코드 이미지가 적층하여 생성되는 광학적 PUF 기반 이미지 큐브는 더욱 높은 보안 수준의 응용에서 간단한 인증 방법으로 위조 방지 기술에 적용될 수 있다.
- [0024] 또한, 본 발명의 실시예에 따르면, 획득되는 광학적 PUF 기반 암호화 코드는 1차원 코드로서, 순차적인 인증 프로세스에도 활용이 가능할 수 있다.
- [0025] 본 발명의 효과는 상기한 효과로 한정되는 것은 아니며, 본 발명의 상세한 설명 또는 청구범위에 기재된 발명의 구성으로부터 추론 가능한 모든 효과를 포함하는 것으로 이해되어야 한다.

도면의 간단한 설명

- [0026] 도 1은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법을 나타낸 흐름도이다.
- 도 2는 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서, 굴절률 이방성 소재, 기본 이미지 및 이진코드 이미지를 나타낸 사진이다.
- 도 3은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 교차 편광판 및 굴절률 이방성 소재의 배치예를 나타낸 예시도이다.
- 도 4는 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서, 교차 편광판 각도에 따른 기본 이미지 및 이진코드 이미지를 나타낸 것이다.
- 도 5는 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이진코드 이미지의 각 축에 따른 엔트로피를 나타낸 그래프이다.
- 도 6은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 생성되는 이미지 큐브를 나타낸 것이다.
- 도 7은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이미지 큐브의 엔트로피를 나타낸 그래프이다.
- 도 8은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이미지 큐브의 intra-HD 및 inter-HD를 나타낸 그래프이다.
- 도 9는 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이미지 큐브 중에 선정되는 2차원의 면을 설명하기 위한 예시도이다.
- 도 10은 도 9에서 선정되는 2차원의 면에서 광학적 PUF 기반 암호화 코드를 생성하는 예를 설명하기 위한 예시도이다.
- 도 11은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이미지 큐브에서 선택되는 3차원 도형을 나타낸 예시도이다.
- 도 12는 도 11에서 선택되는 3차원 도형의 각 면에서 광학적 PUF 기반 암호화 코드를 생성하는 예를 설명하기 위한 예시도이다.

발명을 실시하기 위한 구체적인 내용

- [0027] 이하에서는 첨부한 도면을 참조하여 본 발명을 설명하기로 한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 따라서 여기에서 설명하는 실시예로 한정되는 것은 아니다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

- [0028] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결(접속, 접촉, 결합)"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 부재를 사이에 두고 "간접적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 구비할 수 있다는 것을 의미한다.
- [0029] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [0030] 그리고, 이 방법은 명확성을 위해 일련의 번호가 붙여진 단계로 묘사되어 있지만 번호 순서가 각 단계의 순서를 지정하는 것은 아니다. 이들 단계 중 일부는 스킵되거나, 병렬로 수행되거나, 엄격히 전후 순서를 유지할 필요 없이 수행될 수 있다. 그러나, 일반적으로 이 방법은 표시된 단계의 번호 순서에 따라 진행된다.
- [0031] 이하 첨부된 도면을 참고하여 본 발명의 실시예를 상세히 설명하기로 한다.
- [0032] 도 1은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법을 나타낸 흐름도이고, 도 2는 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서, 굴절률 이방성 소재, 기본 이미지 및 이진 코드 이미지를 나타낸 사진이다.
- [0033] 도 1 및 도 2에서 보는 바와 같이, 광학적 PUF 기반 암호화 코드 획득 방법은 소재 마련단계(S110), 기본 이미지 획득단계(S120), 이진코드 이미지 생성단계(S130), 이미지 큐브 생성단계(S150) 및 암호화 코드 생성단계(S170)를 포함할 수 있다.
- [0034] 여기서, 소재 마련단계(S110)는 굴절률 이방성 소재(200)를 마련하는 단계일 수 있다.
- [0035] 그리고, 기본 이미지 획득단계(S120)는 굴절률 이방성 소재에 빛을 투과시키고, 굴절률 이방성 소재를 투과한 빛을 수광하여 간섭 패턴(310)을 가지는 기본 이미지(300)를 획득하는 단계일 수 있다.
- [0036] 또한, 이진코드 이미지 생성단계(S130)는 간섭 패턴(310)에 대응되는 이진코드를 가지는 이진코드 이미지(400)를 생성하는 단계일 수 있다.
- [0037] 그리고, 이미지 큐브 생성단계(S150)는 복수개의 이진코드 이미지를 적층하여 이미지 큐브를 생성하는 단계일 수 있다.
- [0038] 또한, 암호화 코드 생성단계(S170)는 이미지 큐브에서 복수 개의 이진코드 이미지를 포함하는 면을 선정하고, 선정된 면에서 이진코드를 추출하여 광학적 PUF 기반 암호화 코드를 생성하는 단계일 수 있다.
- [0039] 이러한 방법에 의해 생성되는 광학적 PUF 기반 암호화 코드는 물리적으로 복제할 수 없는 형태이다. 따라서, 광학적 PUF 기반 암호화 코드는 더욱 높은 보안 수준의 응용에서 간단한 인증 방법으로 위조 방지 기술에 적용될 수 있다.
- [0040] 상세히, 소재 마련단계(S110)는 굴절률 이방성 소재(200)를 마련하는 단계일 수 있다.
- [0041] 여기서, 굴절률 이방성 소재(200)는 배향 공정을 거치지 않은 액정성 소재일 수 있다. 예를 들면, 굴절률 이방성 소재(200)는 배향 공정을 거치지 않은 액정이거나, 또는 배향 공정을 거치지 않은 액정성 고분자일 수 있다.
- [0042] 굴절률 이방성 소재(200)는 주름(210)을 가질 수 있으며, 광학적 비등방성을 가질 수 있다. 주름(210)은 굴절률 이방성 소재가 경화되어 형성될 수 있다.
- [0043] 기본 이미지 획득단계(S120)는 굴절률 이방성 소재(200)에 빛을 투과시키고, 굴절률 이방성 소재(200)를 투과한 빛을 수광하여 간섭 패턴(310)을 가지는 기본 이미지(300)를 획득하는 단계일 수 있다.
- [0044] 기본 이미지 획득단계(S120)에서, 기본 이미지(300)는 굴절률 이방성 소재(200)를 사이에 두고 배치되는 교차 편광판을 통과한 빛을 수광하여 획득될 수 있다.
- [0045] 도 3은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 교차 편광판 및 굴절률 이방성 소재의 배치예를 나타낸 예시도이다.
- [0046] 도 3을 더 포함하여 보는 바와 같이, 굴절률 이방성 소재(200)는 한 쌍의 교차 편광판(510, 520)의 사이에 배치

될 수 있다. 광원(500)에서 방출되는 빛(501)은 한 쌍의 교차 편광판(510,520) 중 전방의 교차 편광판(510)을 통과한 후 굴절률 이방성 소재(200)를 통과하고 다시 후방의 교차 편광판(520)을 통과한 후 수광부(530)에 수광될 수 있다. 그리고 수광부(530)에 수광되는 빛으로부터 기본 이미지(300)가 획득될 수 있다.

- [0047] 기본 이미지(300)의 간섭 패턴(310)은 굴절률 이방성 소재(200)의 주름(210)에 대응되게 형성될 수 있는데, 액정이 배향공정을 거치지 않았기 때문에, 주름(210)의 형태는 무작위(Random)일 수 있으며, 따라서, 간섭 패턴(310)도 무작위로 형성될 수 있다.
- [0048] 빛의 투과율은 액정의 방향에 따라 결정될 수 있기 때문에, 간섭 패턴(310)은 교차 편광판(510,520) 사이에서 빛의 밝기가 무작위함에 기인하여 형성될 수 있다.
- [0049] 그리고, 기본 이미지(300)는 굴절률 이방성 소재(200)를 기준으로 교차 편광판(510,520)의 회전 각도에 따라 무작위한 간섭 패턴을 가질 수 있다. 다시 말하면, 교차 편광판의 각도를 변경할 때 마다 굴절률 이방체로 기반 랜덤 주름의 빛의 투과도 또한 달라지므로 간섭 패턴을 통해 얻은 이진코드 또한 달라질 수 있다.
- [0050] 도 4는 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서, 교차 편광판 각도에 따른 기본 이미지 및 이진코드 이미지를 나타낸 것이다.
- [0051] 도 4에서 보는 바와 같이, 교차 편광판(510,520)의 각도가 5° 단위로 회전되어 마련되면 획득되는 기본 이미지의 간섭 패턴(310)은 서로 다르게 형성됨을 확인할 수 있다. 여기에서는 교차 편광판(510,520)의 회전 각도가 5° 단위로 달라지는 경우의 기본 이미지를 예로 설명하고 있지만, 회전 각도가 1° 단위로 달라지더라도 획득되는 기본 이미지의 간섭 패턴(310)은 서로 다르게 형성될 수 있다.
- [0052] 다시 도 1 내지 도 4를 참조하면, 이진코드 이미지 생성단계(S130)는 간섭 패턴(310)에 대응되는 이진코드를 가지는 이진코드 이미지(400)를 생성하는 단계일 수 있다.
- [0053] 이진코드 이미지 생성단계(S130)에서, 이진코드는 기본 이미지(300)의 간섭 패턴(310)이 알고리즘 필터링되어 생성될 수 있다. 이진코드 이미지(400)는 생성되는 이진코드의 이미지일 수 있다.
- [0054] 이진코드는 "0", "1"로 설정될 수 있다. 이진코드는 도 2의 (c)에서와 같이 액정의 주름을 닮은 자연스러운 형태로 형성될 수 있다. 즉, 이진코드 이미지(400)에서 흰색 부분이 "0"이고, 검은 부분이 "1"인 경우, 이진코드 이미지(400)를 작은 크기의 픽셀로 구분할수록 액정의 주름을 닮은 자연스러운 형태로 형성될 수 있다. 그리고, 동일한 크기의 이진코드 이미지에 포함되어 있는 이진코드의 개수도 증가하기 때문에, 더욱 상세한 이진코드를 가질 수 있다.
- [0055] 한편, 생성되는 이진코드 이미지(400)에 대한 연산 처리 속도 등을 고려하였을 때, 이진코드는 사각 픽셀로 단 순화된 형태로 좀 더 단순화되어 생성될 수도 있다.
- [0056] 이진코드 이미지(400)의 이진코드는 기본 이미지(300)의 간섭 패턴(310)에 대응되어 형성되기 때문에, 도 4에서와 같이, 교차 편광판의 회전 각도에 따라 다른 형태의 간섭 패턴을 가지는 기본 이미지에 의해, 각각의 기본 이미지에 대응하여 생성되는 이진코드 이미지(400)의 이진코드 또한 각각 다르게 형성될 수 있다.
- [0057] 광학적 PUF 기반 암호화 코드 획득 방법은 이진코드 이미지 검증단계(S140)를 포함할 수 있다.
- [0058] 이진코드 이미지 검증단계(S140)는 이진코드를 기초로 이진코드 이미지의 무작위성을 검증하는 단계일 수 있다.
- [0059] 도 5는 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이진코드 이미지의 각 축에 따른 엔트로피를 나타낸 그래프이다.
- [0060] 새넌 엔트로피(Entropy) 방정식을 활용하여 측정되는 엔트로피는 이진코드의 "0", "1"로 설정될 확률이 계산되어 표현되는 것으로 무작위성의 척도일 수 있다.
- [0061] 엔트로피 측정을 위해 사용되는 이진코드 이미지는 250 픽셀 × 250 픽셀로 총 62,500개의 비트(Bit)로 구성되었다.
- [0062] 그리고, 표준 방정식을 사용하여 이진코드의 행(Row)(X축)과 열(Column)(Y축)을 따라 엔트로피(Ex,y)를 측정하였다. 여기서, Ex,y는 각 축을 따라 "1"로 설정될 확률로 정의된다.
- [0063] x축을 따른 평균 엔트로피(Ex)는 0.9894±0.02로 측정되었고(도 5의 (a) 참조), y축을 따른 평균 엔트로피(Ey)는 0.9877±0.03로 측정되었다(도 5의 (b) 참조). 이는 완전 무작위성에 가까운 1의 값에 근접하므로 이진코드

는 완전 무작위성이 있음을 확인할 수 있다.

- [0064] 도 6은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 생성되는 이미지 큐브를 나타낸 것이고, 도 7은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이미지 큐브의 엔트로피를 나타낸 그래프이고, 도 8은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이미지 큐브의 intra-HD 및 inter-HD를 나타낸 그래프이다.
- [0065] 도 1과 함께, 도 6 내지 도 8에서 보는 바와 같이, 이미지 큐브 생성단계(S150)는 복수개의 이진코드 이미지(400)를 적층하여 이미지 큐브(600)를 생성하는 단계일 수 있다.
- [0066] 이미지 큐브 생성단계(S150)에서 복수개의 이진코드 이미지(400)는 Z축 방향으로 적층되어 형성될 수 있다. 이미지 큐브(600)는 그 자체가 랜덤한 3차원의 데이터일 수 있다. 이미지 큐브(600)에서 X축과 Y축 면의 데이터 또한 무작위일 수 있다.
- [0067] 광학적 PUF 기반 암호화 코드 획득 방법은 이미지 큐브 검증단계(S160)를 포함할 수 있다.
- [0068] 이미지 큐브 검증단계(S160)는 이미지 큐브(600)의 무작위성 및 유일성을 검증하는 단계일 수 있다.
- [0069] 먼저, 이미지 큐브(600)의 무작위성을 검증하기 위해서, 여기에서도, 새넨 엔트로피 방정식을 활용하여 이미지 큐브(600)의 엔트로피가 측정될 수 있다.
- [0070] 엔트로피 측정을 위해 사용되는 이미지 큐브(600)는 250 픽셀 × 250 픽셀 × 250 픽셀 사이즈로 구성되었다. 이미지 큐브(600)의 엔트로피는 이미지 큐브(600)의 각 비트(bit)가 "1"로 설정될 확률에 의해 0.9912 ± 0.02 로 측정되었다. 이는 완전 무작위성에 가까운 1의 값에 근접하므로 이진코드는 완전 무작위성이 있음을 확인할 수 있다(도 7 참조).
- [0071] 그리고, 이미지 큐브(600)의 유일성 및 신뢰성을 검증하기 위해서, 해밍 거리(Hamming Distance, 이하 'HD'라 한다)가 측정될 수 있다.
- [0072] HD는 해당 비트 위치에서 동일하지 않은 비트의 수로 정의되는 유사성의 척도이다. 예를 들어 '110010'과 '101011' 사이의 HD는 3이 된다.
- [0073] HD는 같은 샘플의 간섭 패턴으로 형성한 이미지 큐브를 여러 번 측정하여 계산하는 내부 해밍 거리(intra-HD, 이하 'intra-HD'라 한다)와, 다른 샘플의 간섭 패턴으로 복수 회 측정하여 계산되는 상호 해밍 거리(inter-HD, 이하 'inter-HD'라 한다)가 있다.
- [0074] 같은 샘플의 간섭 패턴으로 여러 번 측정하여 계산하는 intra-HD의 값은 이상적으로 0이 나와야 한다.
- [0075] 이를 위해, 하나의 이미지 큐브를 복수 회 측정하였다. 구체적으로, 1개의 이미지 큐브를 사용하여 70개의 응답(Response) intra-HD를 측정하였다. 이 결과, intra-HD는 0.0512 였다.
- [0076] 그리고, 다른 샘플의 간섭 패턴으로 여러 번 측정하여 계산하는 상호 해밍 거리(inter-HD)의 값은 이상적으로 0.5가 나와야 한다.
- [0077] 이를 위해, 서로 다른 이미지 큐브를 복수 회 측정하였다. 구체적으로, 서로 다른 70개의 이미지 큐브를 사용하여 inter-HD를 측정하였다. 이 결과, inter-HD는 0.4989 였다.
- [0078] 즉, 측정 결과 intra-HD는 0.0512로서 이상적인 값인 0에 근접하고, inter-HD는 0.4989로서 이상적인 값인 0.5에 근접하므로 이진코드는 유일성과 신뢰성이 있음을 확인하였다(도 8 참조).
- [0079] 이와 같이, 이진코드 이미지의 무작위성과, 이미지 큐브의 무작위성, 유일성 및 신뢰성이 검증된 바, 이미지 큐브를 이용하여 획득되는, 후술할 광학적 PUF 기반 암호화 코드는 높은 보안 수준에서 위조 방지 기술에 적용될 수 있다.
- [0080] 도 9는 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이미지 큐브 중에 선정되는 2차원의 면을 설명하기 위한 예시도이고, 도 10은 도 9에서 선정되는 2차원의 면에서 광학적 PUF 기반 암호화 코드를 생성하는 예를 설명하기 위한 예시도이다.
- [0081] 도 1, 도 6, 도 9 및 도 10에서 보는 바와 같이, 암호화 코드 생성단계(S170)는 이미지 큐브(600)에서 복수 개의 이진코드 이미지(400)를 포함하는 면을 선정하고, 선정된 면에서 이진코드를 추출하여 광학적 PUF 기반 암호화 코드를 생성하는 단계일 수 있다.

- [0082] 암호화 코드 생성단계(S170)에서, 면은 이미지 큐브(600) 중의 무작위로 선정되는 3개의 점에 의해 형성되는 2차원의 면일 수 있다.
- [0083] 그리고, 2차원의 면은 이미지 큐브(600)에서 복수 개의 이진코드 이미지가 적층되어 형성되는 적층 표면에서 선정되는 것일 수 있다. 여기서, 적층 표면은 복수 개의 이진코드 이미지로 형성되는 표면일 수 있다. 즉, 적층 표면은 이미지 큐브(600)의 측면 표면일 수 있다. 따라서, 도 9의 (a)에는 두 개의 적층 표면(601,602)이 도시되었지만, 가려져서 보이지 않는 두 개의 적층 표면이 더 있다.
- [0084] 도 9의 (a)에서, 우측의 적층 표면(601)에서 3개의 점(P1,P2,P3)에 의해 형성되는 2차원의 면(610)이 선정되면, 선정된 2차원의 면(610)에서 이진코드가 추출되어 광학적 PUF 기반 암호화 코드(700)가 생성될 수 있다(도 10 참조).
- [0085] 즉, 선정된 2차원의 면(610)은 Y-Z 평면상의 면이 되고, 선정된 2차원의 면(610)은 적층된 복수개의 이진코드 이미지의 이진코드 중, Y-Z 평면상에서의 이진코드에 의해 새로운 이진코드를 형성할 수 있다. 광학적 PUF 기반 암호화 코드(700)는 선정된 2차원의 면(610)이 Y-Z 평면상에 가지는 새로운 이진코드가 추출되어 생성될 수 있다.
- [0086] 광학적 PUF 기반 암호화 코드(700)는 예를 들면, 2차원의 면(610)에서 열을 바꿔가면서 행방향을 따라 순차적으로 추출되는 이진코드로 이루어질 수 있다.
- [0087] 여기서, 추출되는 이진코드는 미리 설정된 알고리즘을 통해 광학적 PUF 기반 암호화 코드(700)로 재구성될 수 있게 된다. 광학적 PUF 기반 암호화 코드(700)는 1차원 코드일 수 있다. 다시 말하면, 광학적 PUF 기반 암호화 코드(700)는 2차원의 면(610)에 저장되어 있는 2차원적인 이진코드를 1차원적으로 푼 것일 수 있다.
- [0088] 1차원 코드는 "0" 또는 "1"에 편향되지 않은 분포를 보여주어 보안성이 높을 수 있다. 따라서, 광학적 PUF 기반 암호화 코드(700)는 보안 기술, 위조 방지기술 및 액세스 제어 시스템과 같은 다양한 보안 관련 분야에 응용될 수 있다.
- [0089] 마찬가지로 방법으로, 도 9의 (a)에서, 좌측의 적층 표면(602)에서 3개의 점(P4,P5,P6)에 의해 형성되는 2차원의 면(620)이 선정되면, 선정된 2차원의 면(620)은 X-Z 평면상에서의 새로운 이진코드를 가지게 되며, 이러한 새로운 이진코드가 추출되어 또 다른 광학적 PUF 기반 암호화 코드가 생성될 수 있다.
- [0090] 3개의 점에 의해 적층 표면에서 형성되는 면의 크기, 위치, 형상을 다양하게 선정함으로써, 새로운 이진코드를 가지는 면이 얻어질 수 있다. 이를 통해 무수히 많은 면을 얻을 수 있어, 무작위성, 유일성 및 신뢰성을 가지는 광학적 PUF 기반 암호화 코드를 얻을 수 있다.
- [0091] 그리고, 도 9의 (b)에서 보는 바와 같이, 암호화 코드 생성단계(S170)에서, 이미지 큐브(600) 중의 무작위로 선정되는 3개의 점에 의해 형성되는 2차원의 면은 이미지 큐브(600)의 내부에서 선정될 수도 있다.
- [0092] 이 경우, 형성되는 2차원의 면은 동일한 X-Y 평면상의 면이 아니도록 선정될 수 있다. 이를 위해, 3개의 점(P7,P8,P9)은 동일한 X-Y 평면상에 위치되지 않도록 선정될 수 있다. 3개의 점(P7,P8,P9)에 의해 형성되는 2차원의 면(630)은 비스듬하게 기울어지거나, 또는 수직한 형태일 수 있다.
- [0093] 한편, 암호화 코드 생성단계(S170)에서, 면은 이미지 큐브(600) 중의 무작위로 선정되는 4개 이상의 점에 의해 형성되는 3차원 도형의 표면 중 하나 이상일 수 있다.
- [0094] 도 11은 본 발명의 일실시예에 따른 광학적 PUF 기반 암호화 코드 획득 방법에서 이미지 큐브에서 선택되는 3차원 도형을 나타낸 예시도이고, 도 12는 도 11에서 선택되는 3차원 도형의 각 면에서 광학적 PUF 기반 암호화 코드를 생성하는 예를 설명하기 위한 예시도이다.
- [0095] 도 11 및 도 12에서 보는 바와 같이, 이미지 큐브(600) 중에 무작위의 4개의 점(P11,P12,P13,P14)이 선정되면, 선정된 4개의 점(P11,P12,P13,P14)에 의해 3차원의 도형(640)이 형성될 수 있다. 그리고, 4개의 점으로 형성되는 3차원의 도형(640)은 4개의 표면(641,642,643,644)을 가질 수 있다. 암호화 코드 생성단계(S170)에서 사용되는 면은 4개의 표면(641,642,643,644) 중 하나 이상일 수 있다. 그리고, 광학적 PUF 기반 암호화 코드(700)는 선정되는 표면으로부터 각각 추출될 수 있다.
- [0096] 광학적 PUF 기반 암호화 코드(710,720,730,740)는 각각의 표면(641,642,643,644)으로부터 획득될 수 있기 때문에, 각각의 광학적 PUF 기반 암호화 코드(710,720,730,740)는 모두 다를 수 있다.

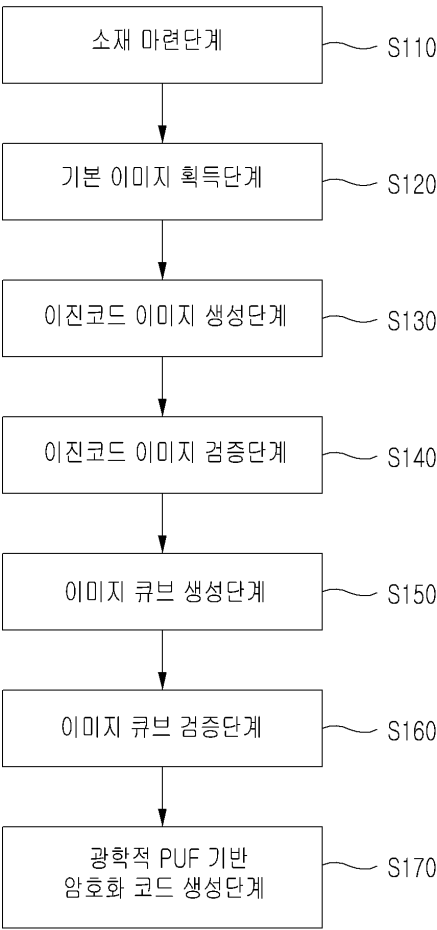
- [0097] 이러한 방법은 단순 2차원의 패스워드가 아닌 3차원 형태의 패스워드로 활용이 가능하도록 도울 수 있다.
- [0098] 이처럼, 본 발명은 액정 분포의 무작위성과 액정의 광학적 효과를 활용하여 지문과 같은 특정 패턴 코드를 형성할 수 있는 광학적 PUF 기반 기본 이미지를 제작할 수 있다.
- [0099] 그리고, 본 발명에 따르면, 기존의 반도체 기반 PUF와 달리 물리적으로 교체하거나 추가 하드웨어 구성요소가 필요 없이 PUF 구성이 가능하다.
- [0100] 또한, 본 발명에 따르면, 광학적 PUF 기반 기본 이미지의 자유형 모양의 무작위한 방향의 주름은 물리적으로 복제할 수 없는 형태이다. 따라서, 광학적 PUF 기반 기본 이미지를 이용하여 생성되는 광학적 PUF 기반 이진코드 이미지와, 이진코드 이미지가 적층하여 생성되는 광학적 PUF 기반 이미지 큐브는 더욱 높은 보안 수준의 응용에서 간단한 인증 방법으로 위조 방지 기술에 적용될 수 있다.
- [0101] 또한, 본 발명에 따라 획득되는 광학적 PUF 기반 암호화 코드는 1차원 코드로서, 순차적인 인증 프로세스에도 활용이 가능할 수 있다.
- [0102] 진술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [0103] 본 발명의 범위는 후술하는 청구범위에 의하여 나타내어지며, 청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

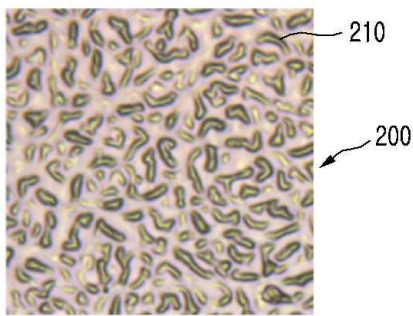
- [0104] 200: 굴절률 이방성 소재
- 210: 주름
- 300: 기본 이미지
- 310: 간섭 패턴
- 400: 이진코드 이미지
- 600: 이미지 큐브
- 610,620,630: 2차원의 면
- 640: 3차원의 도형
- 700: 광학적 PUF 기반 암호화 코드

도면

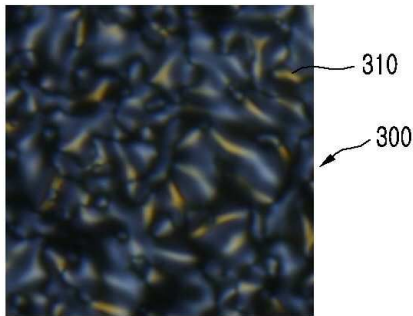
도면1



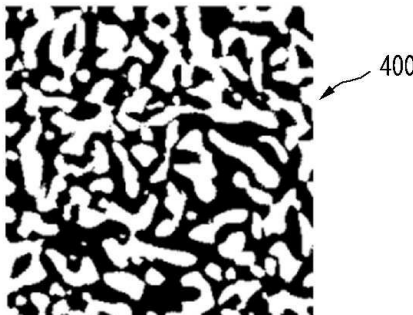
도면2



(a)

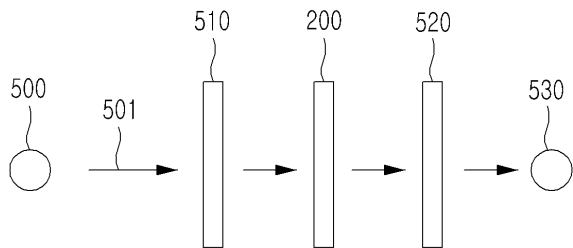


(b)



(c)

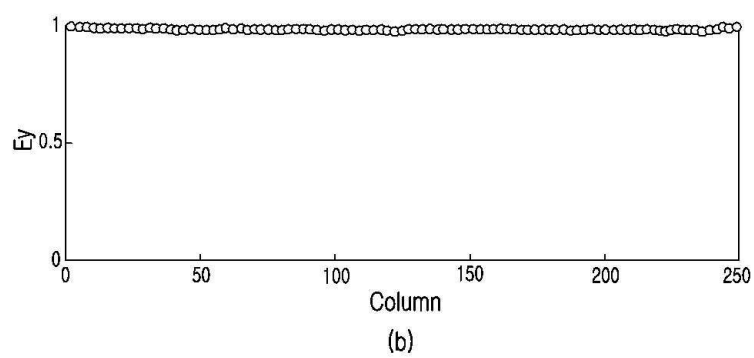
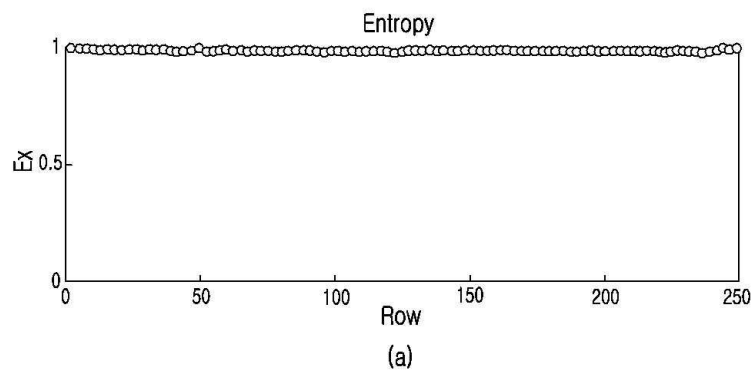
도면3



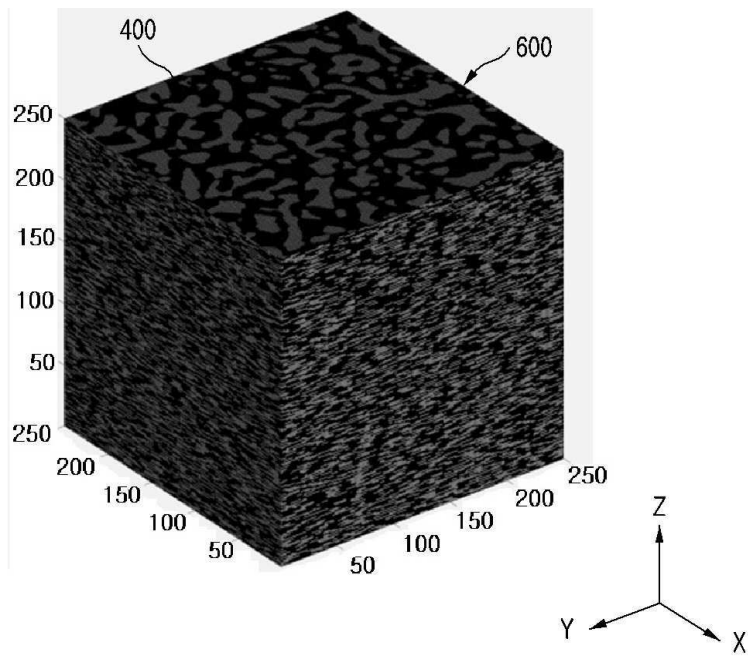
도면4

교차 편광판 각도(°)	0	5	10	15	20	25
간섭 패턴						
이진코드						

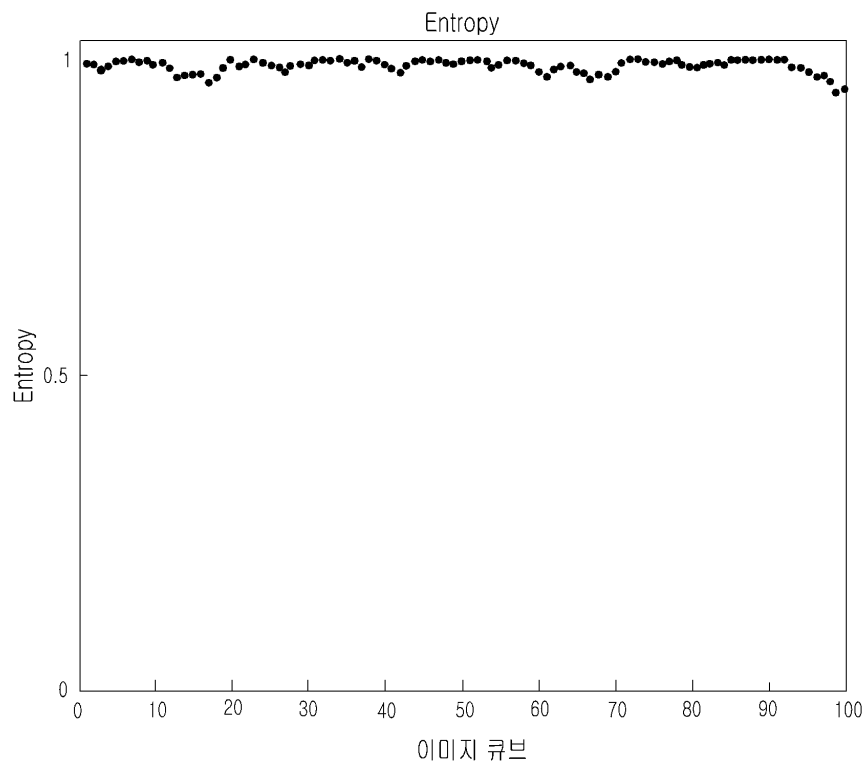
도면5



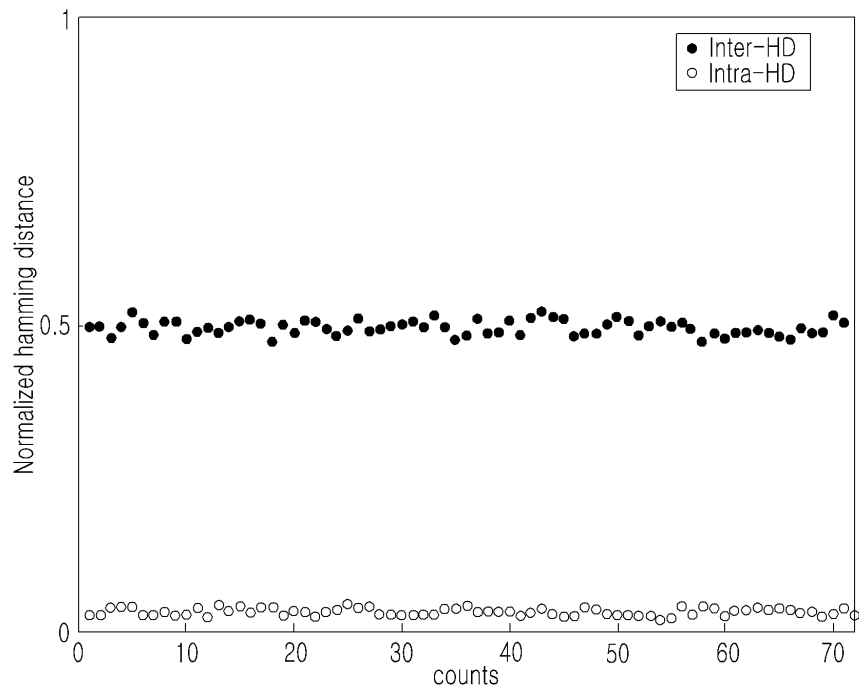
도면6



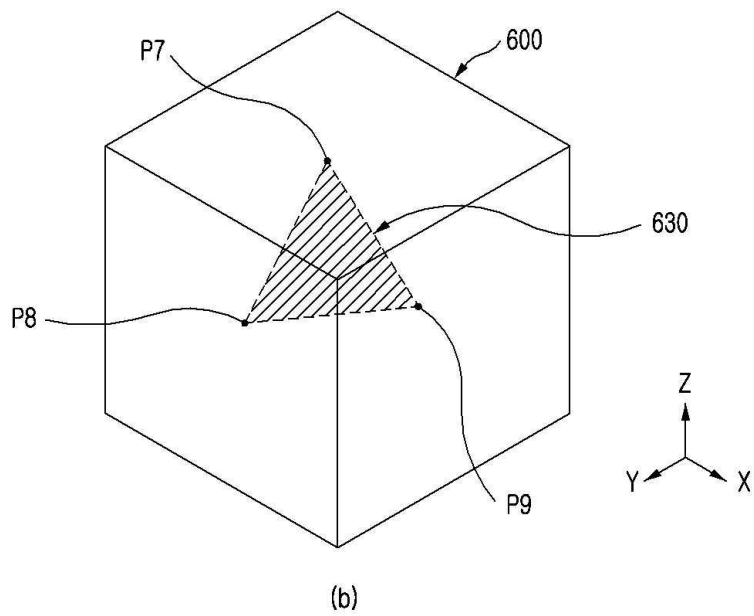
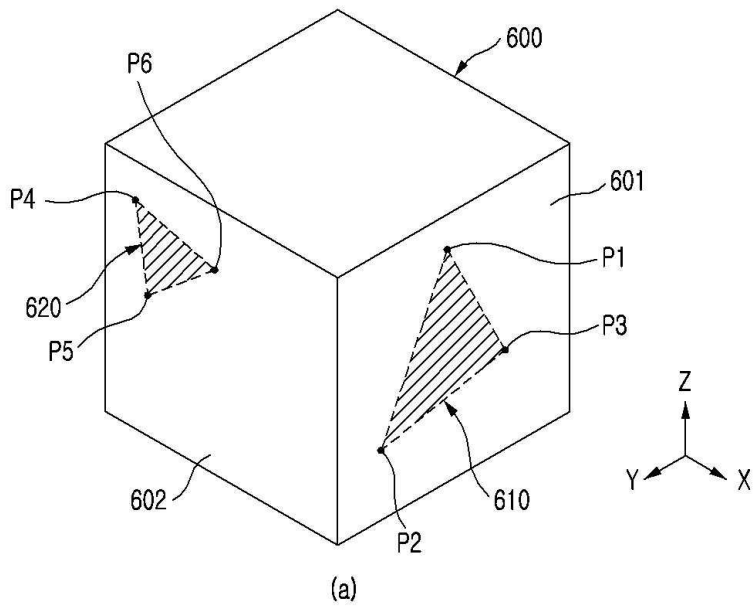
도면7



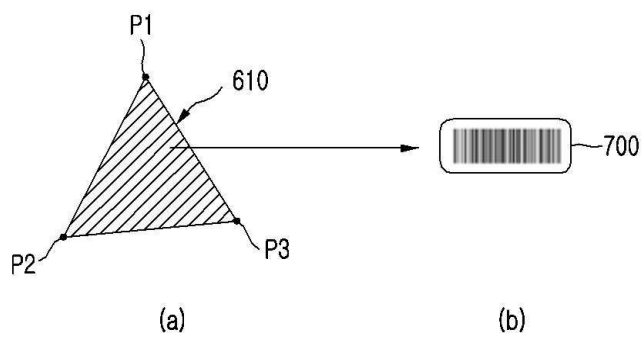
도면8



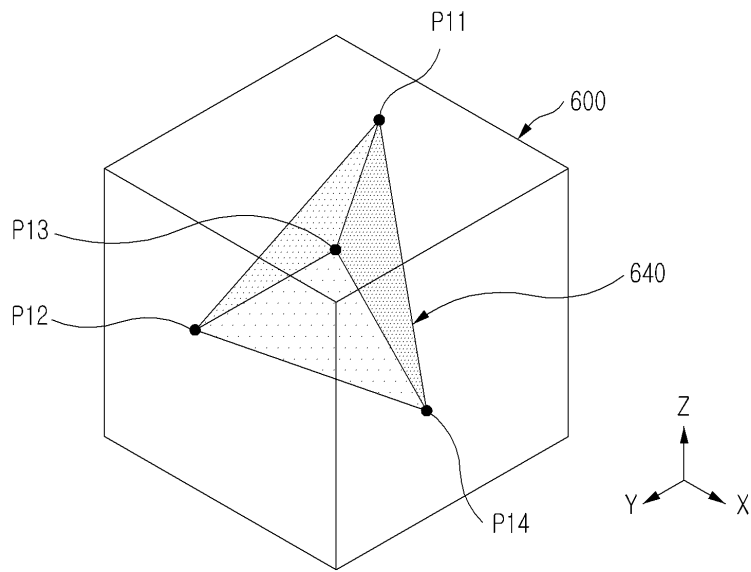
도면9



도면10



도면11



도면12

